Micronet®
Faster and Easier Networks

User's Manual

Wireless Broadband Router

Model No.: SP916GL

http://www.micronet.info

Contents

1 OVERVIEW **1**

1.1 INTRODUCTION 1
1.2 PACKAGE CONTENT 1
1.3 PRODUCT FEATURE 1
Router Mode *1*
Standards *2*
Internet Access *2*
Security Features *2*
Wireless Features *2*
Management Features *2*
1.4 SYSTEM REQUIREMENTS 2
1.5 APPLICATIONS 3

2 GETTING STARTED **3**

2.1 THE FRONT LEDS 3
2.2 THE REAR PORTS 4

3 CONFIGURATION **5**

3.1 CONFIGURING WITH WEB BROWSER 5
3.2 CONFIGURING SYSTEM BASE PARAMETER 6
3.2.1 Host-Name Setting *6*
3.2.2 System Time Setting *6*
3.2.3 Administrator Setting *7*
3.2.4 Firmware Upgrades Setting *7*
3.2.5 Configuration Tools *8*
3.2.6 System Log *8*
3.2.7 System Reset *9*
3.3 WAN CONFIGURATION SETTING 9
3.3.1 Dynamic IP Address: *10*
3.3.2 Static IP Address: *10*
3.3.3 PPPoE: *11*
3.3.4 PPTP: *11*
3.3.5 DNS: *12*
3.3.6 DDNS: *12*
3.4 LAN CONFIGURATION SETTING 13
3.4.1 LAN Configuration: *13*
3.4.2 DHCP Client List: *14*
3.4.3 UPnP configuration: *14*
3.5 WIRELESS CONFIGURATION SETTING 15
3.5.1 Wireless Setting: *15*
3.5.2 Wireless Security Setting: *16*
3.5.3 WDS Configuration Setting: *17*
3.6 NAT CONFIGURATION SETTING 18
3.6.1 Virtual Server Setting: *18*
3.6.2 Port Mapping Setting: *19*
3.6.3 DMZ Setting: *20*
3.7 FIREWALL CONFIGURATION 20
3.7.1 Firewall Setting: *20*
3.7.2 Client Filtering: *21*
3.7.3 MAC Control: *21*
3.8 ROUTE CONFIGURATION 22
3.8.1 Static Routing: *22*
3.8.2 Dynamic Routing: *22*

3.8.3 Routing Table: *23*
3.9 SYSTEM STATUS 23
4 GLOSSARY **24**

1 Overview

1.1 Introduction

Thank you for purchasing Micronet SP916GL Wireless Broadband Router with 4-port Fast Ethernet Switch for cable and DSL application.

SP916GL is the perfect device to connect a small group of PCs to a high-speed Broadband Internet connection or to an Ethernet backbone. Configurable as a DHCP server, SP916GL acts as the only externally recognized Internet device on your local area network (LAN). It could serve as an Internet firewall, protecting your network from being accessed by outside users. In addition, SP916GL supports 64-bit and optional 128-bit Wired Equivalent Privacy (WEP) and WPA/WPA2 (802.1x, TKIP, AES) to protect your WLAN network.

SP916GL offers data rate up to 108Mbps, almost 10 times faster than the widely deployed 802.11b products found in homes, businesses, and public wireless hotspots around the country — but since they share the same 2.4GHz radio band, these devices can also work with existing 11Mbps wireless devices.

This user guide is aimed at easy installation procedures of this device. Before your installation, please read the following procedures carefully.

1.2 Package Content

Before you start installing the product, please verify the following items are in the package：

- Micronet SP916GL Wireless Broadband Router
- Quick Installation Guide
- Manual CD
- One network cable (RJ-45 Category 3 or 5 UTP/STP)
- Power Adapter(9VDC above1.5A)
- External Antenna

1.3 Product Feature

Router Mode

- PPP over Ethernet (RFC-2516)
- DHCP Server and Client
- PPTP Client
- NAPT (Network Address and Port Translation)
- NAT (Network Address Translation)
- ICMP (Internet Control Message Protocol)

Standards

- EEE 802.3 10Base-T Ethernet
- IEEE 802-3u 100Base-TX Fast Ethernet
- IEEE 802.11b, 802.11g, Super-G
- WiFi compliance

Internet Access

- TCP/IP, UDP, ICMP, ARP, RARP, PPPoE, NAT, DHCP (client/server), PPTP client, Static IP assignment

Security Features

- Password protected configuration access
- User authentication (PAP/CHAP) for PPP connection

Wireless Features

- Wireless Frequency Range: 2.400GHz to 2.500GHz
- Wireless Spreading: DSSS (Direct Sequence Spread Spectrum), CCK OFDM, QPSK, BPSK
- Wireless Transmit Power: +15 dBm
- Wireless Security: Supports the Wired Equivalent Privacy (WEP) 64-bit and optional 128-bit, WPA/WPA2 (802.1x, TKIP, AES)
- Wireless Operating Range:

  Open Space : 100-300m
  Indoor : 35-100m

Management Features

- Plug & Play Installation
- Local & Remote Management
- Web-based configuration
- Firmware upgrades
- Alarm Status & Power Indicators
- Event & History log

1.4 System Requirements

- Windows 98, 98SE, Millennium Edition (ME), 2000 and XP operating systems
- Microsoft Internet Explorer 5.5 or above
- DSL/ Cable Modem Broadband Internet connection and ISP account
- PCs equipped with 10Mbps or 10/100 Mbps Ethernet connection to support TCP/IP protocol

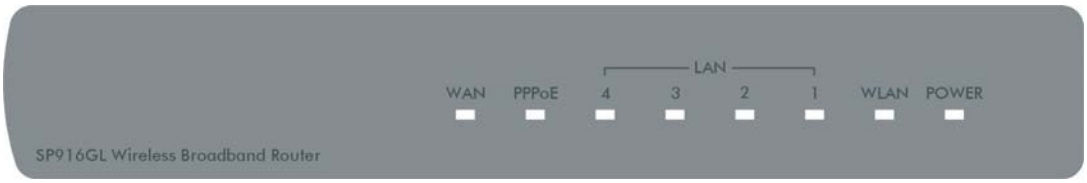
- One RJ-45 Broadband Internet connection
- One PC with an installed 10Mbps, 100Mbps, or 10/100 Mbps Ethernet card
- TCP/IP network protocol for each PC
- UTP network cable with RJ-45 connector

1.5 Applications

- Device sharing and wireless multimedia file transfer
- Wide range wireless office
- Wireless building-to-building data communication
- Built-in infrastructure mode
- Difficult-to-wire environments
- Temporary LANs for scenarios such as trade-exhibitions and meetings
- Frequently changing environments
- Remote access to corporate network information

2 Getting Started

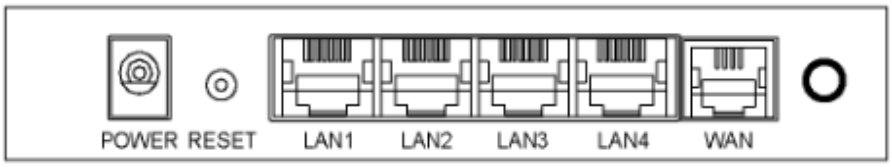
2.1 The Front LEDs



LEDs:

LED	Description
Power	Power is properly connected.
WLAN	Lights on when the wireless works.
LAN(1-4)	If the LED continuously illuminated, the Router is successfully connected to a device through the corresponding port (1, 2, 3 or 4). If the LED is flashing, the Router is actively sending or receiving data over that port.
PPPoE	In dynamic or fixed IP mode, it indicates WAN Ethernet connection speed. In PPPoE mode, it indicates PPPoE connection status.
WAN	The WAN illuminates when the Router is powered on and flashes when the Router is actively sending or receiving data over the WAN network.

2.2 The Rear Ports



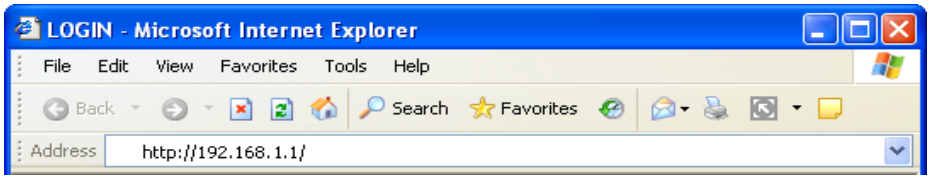
Connector	Description
Power	Plug in the power adapter to connect to the power outlet
Reset Switch	Press until reboot will restore router to default settings..
LAN (1-4)	For connecting to your networked devices, such as PCs, print servers, remote hard drives, and anything else you want to put on your network.
WAN	Forl connecting to your cable, DSL modem or Ethernet backbone.

3 Configuration

3.1 Configuring with Web Browser

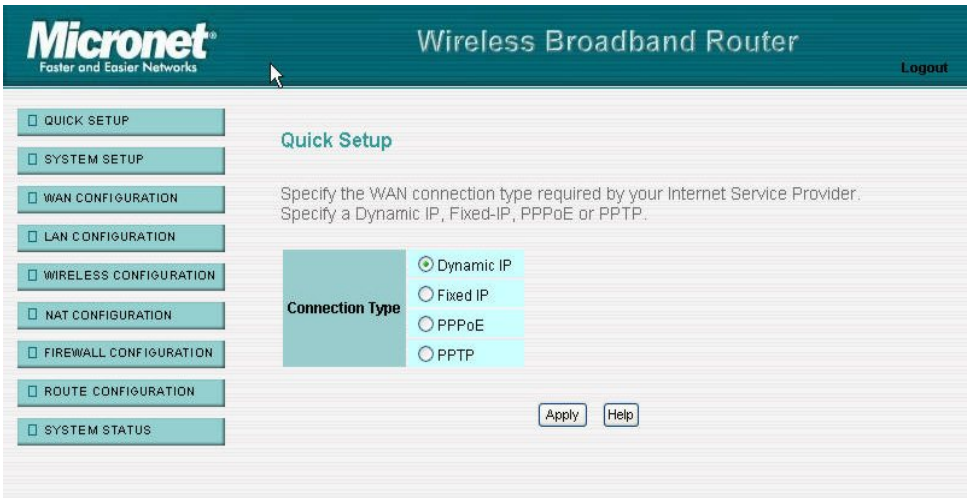
In order to communicate with this Wireless Router, you have to configure the IP addresses of your computer to be compatible with the device. It is advisable to change the administrator password to safeguard your network.

Step1. To configure the router, open your browser, type 'http: //192.168.1.1' into the address bar and click '**Go**' to get to the login page. Save this address in your Favorites for future reference.



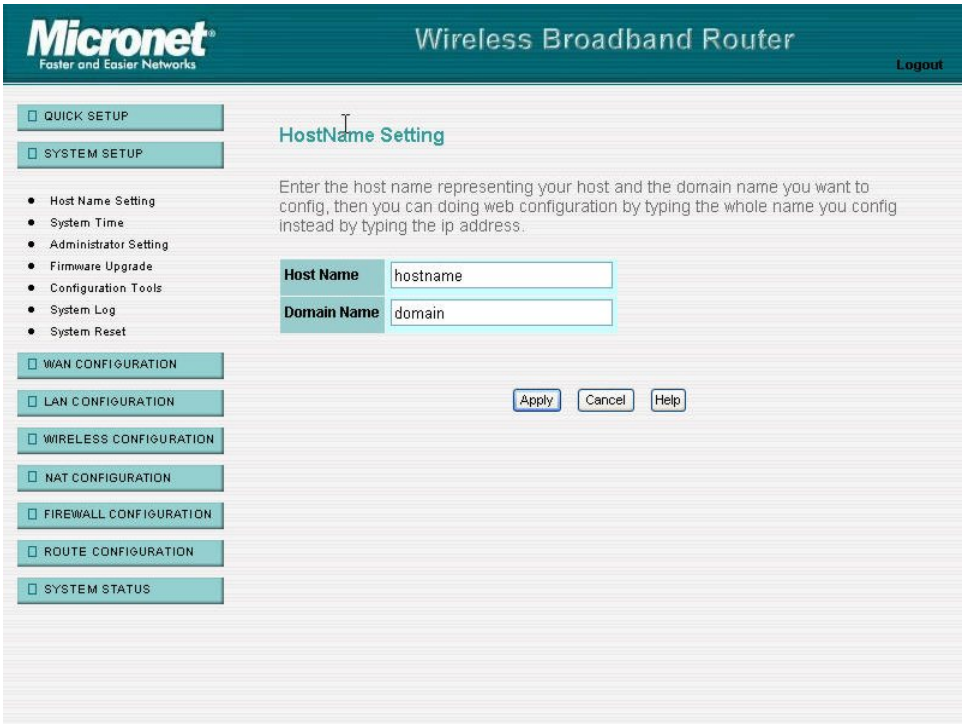
Step2. At the Password prompt, type '**admin**'. You can change these later if you wish. Click '**LOGIN**'.

Step3. Select "**Quick Setup**" for easier configuration to set up the Router.



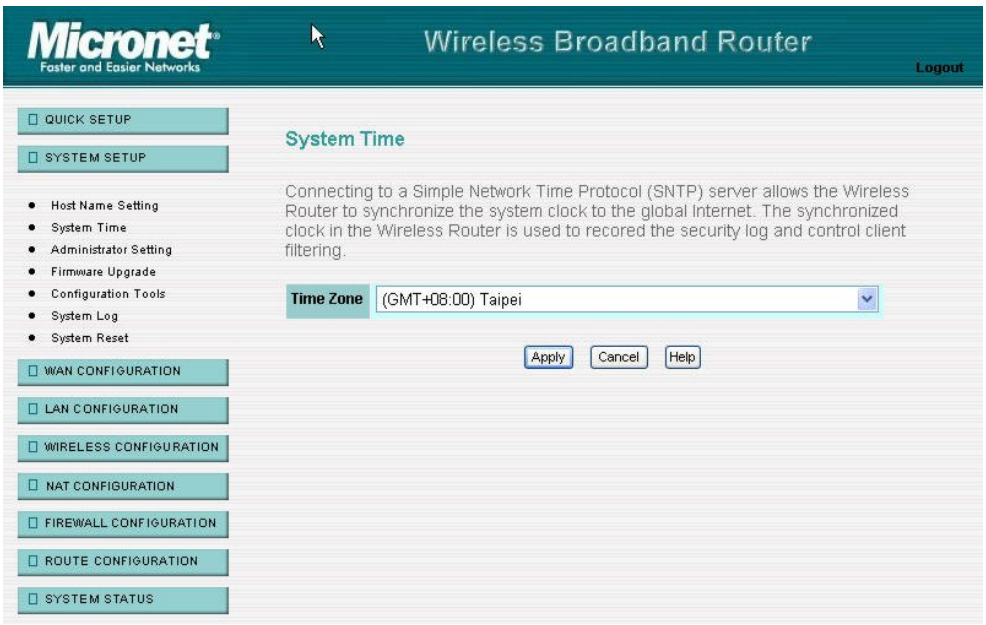
3.2 Configuring System Base parameter

3.2.1 Host-Name Setting



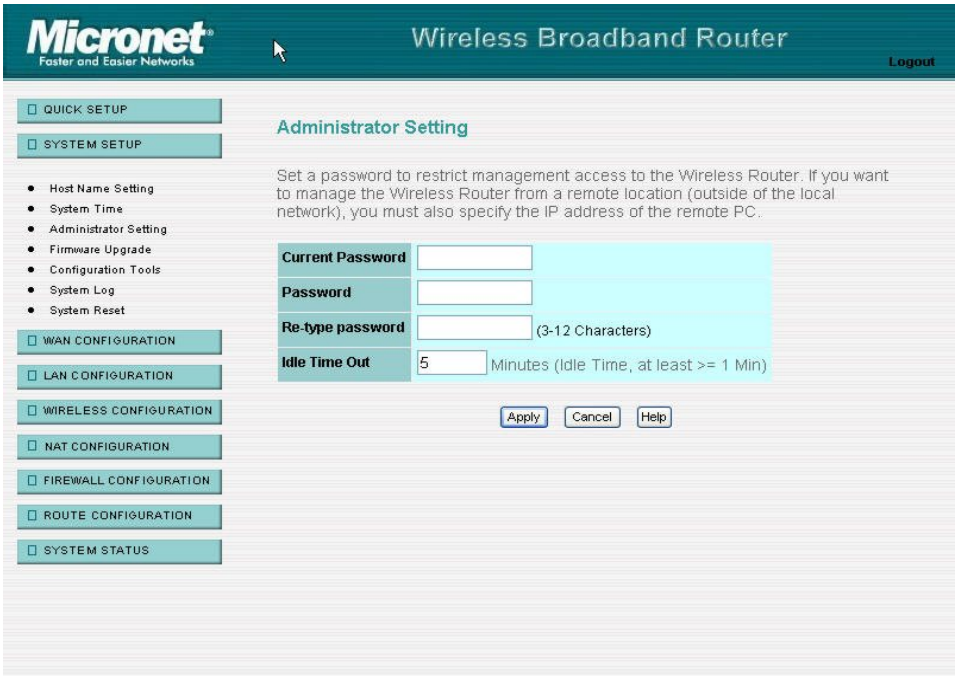
Enter the "**Host Name**" representing your host and the "**Domain Name**". If you want to configure, then you can do web configuration by typing in the whole name which you want to configure instead of typing the IP address.

3.2.2 System Time Setting



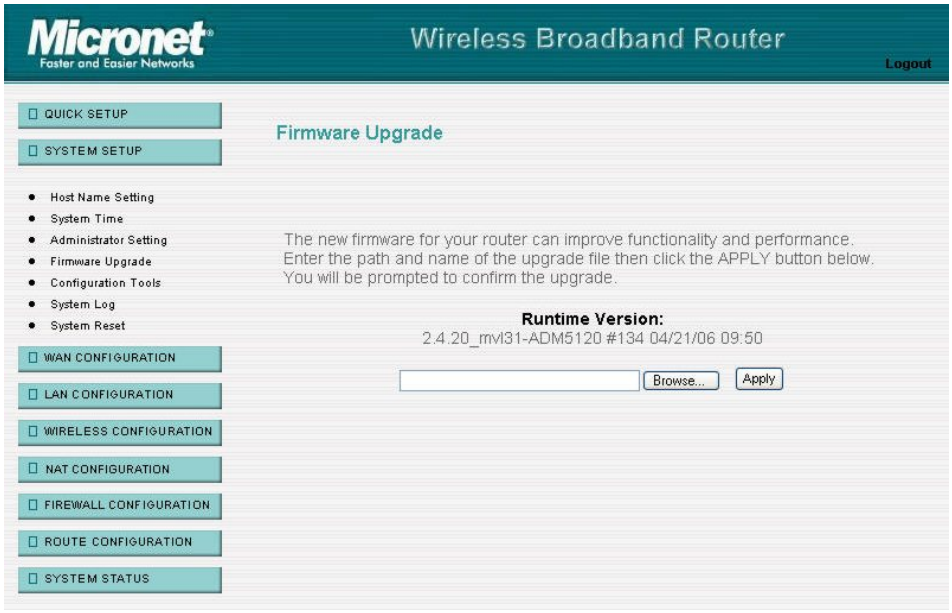
Connecting to a **Simple Network Time Protocol (SNTP) server** allows the SP916GL to synchronize the system clock to the global Internet. The synchronized clock is used to record the security log and control client filtering.

3.2.3 Administrator Setting



Set a password to restrict management access to the SP916GL. The default is "**admin**".

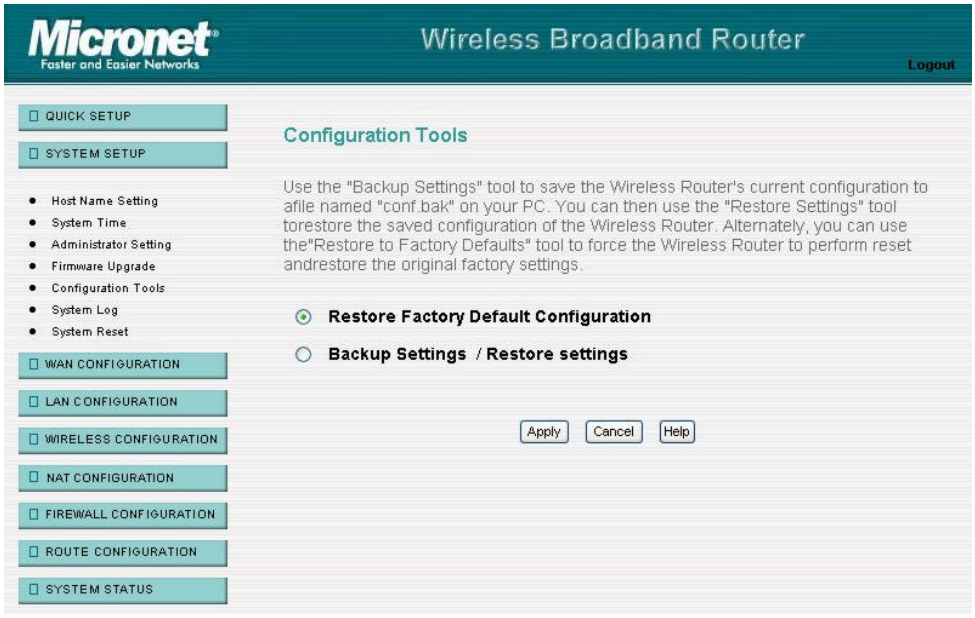
3.2.4 Firmware Upgrades Setting



The new firmware for SP916GL can improve functionality and performance.

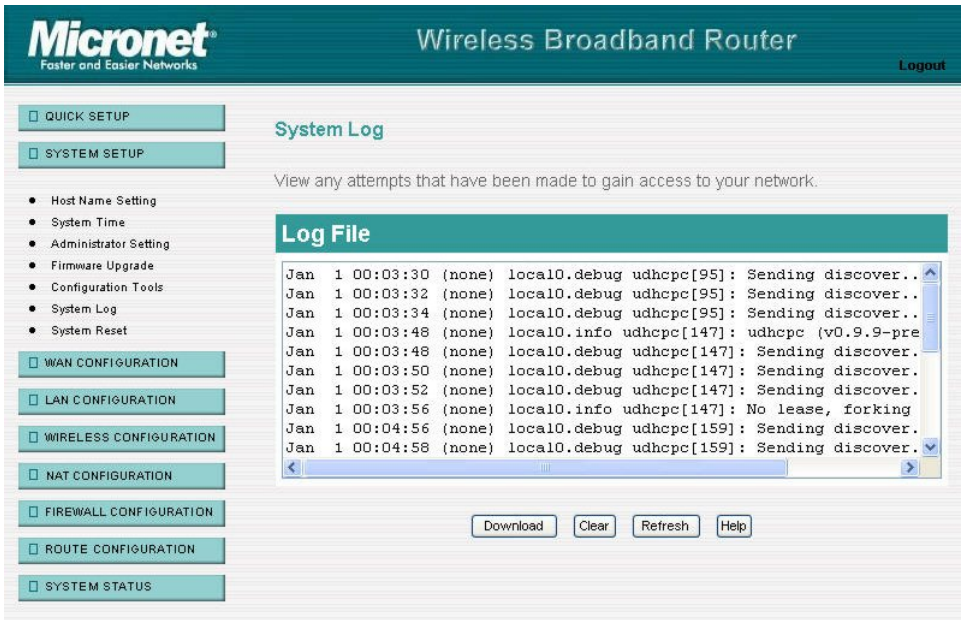
Enter the path and name of the upgrade file then click the “**Apply**” button below. You will be prompted to confirm the upgrade.

3.2.5 Configuration Tools


Micronet
Faster and Easier Networks
Wireless Broadband Router
Logout
QUICK SETUP
SYSTEM SETUP
Host Name Setting
System Time
Administrator Setting
Firmware Upgrade
Configuration Tools
System Log
System Reset
WAN CONFIGURATION
LAN CONFIGURATION
WIRELESS CONFIGURATION
NAT CONFIGURATION
FIREWALL CONFIGURATION
ROUTE CONFIGURATION
SYSTEM STATUS
Configuration Tools
Use the "Backup Settings" tool to save the Wireless Router's current configuration to a file named "conf.bak" on your PC. You can then use the "Restore Settings" tool to restore the saved configuration of the Wireless Router. Alternately, you can use the "Restore to Factory Defaults" tool to force the Wireless Router to perform reset and restore the original factory settings.
Restore Factory Default Configuration
Backup Settings / Restore settings
Apply
Cancel
Help

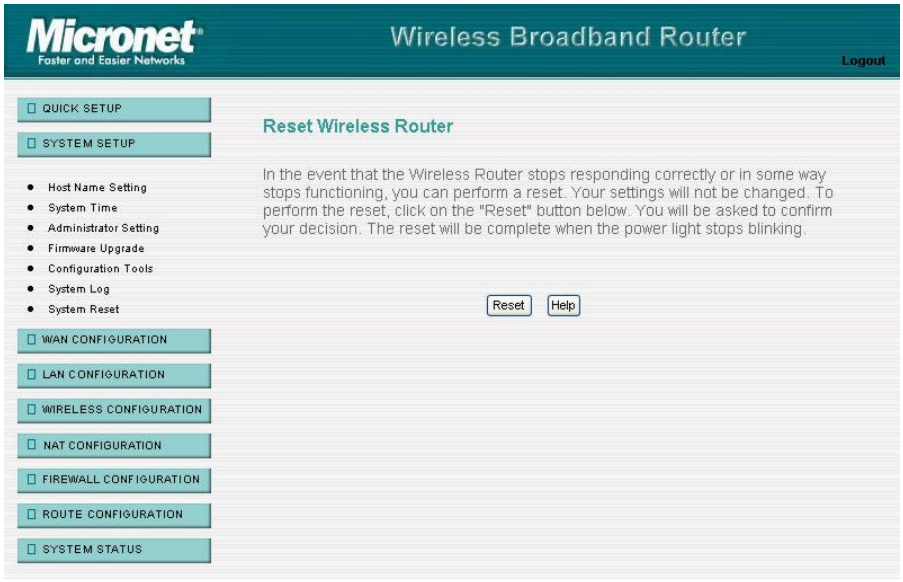
Selecting “**Restore Factory Default Configuration**” will force SP916GL to return and restore the original factory settings. Selecting “**Backup settings tool/ Restore Settings**” will save the SP916GL current configuration to a file named “**conf.bak**” on console PC. You could then use the tool to restore the saved configuration of SP916GL.

3.2.6 System Log



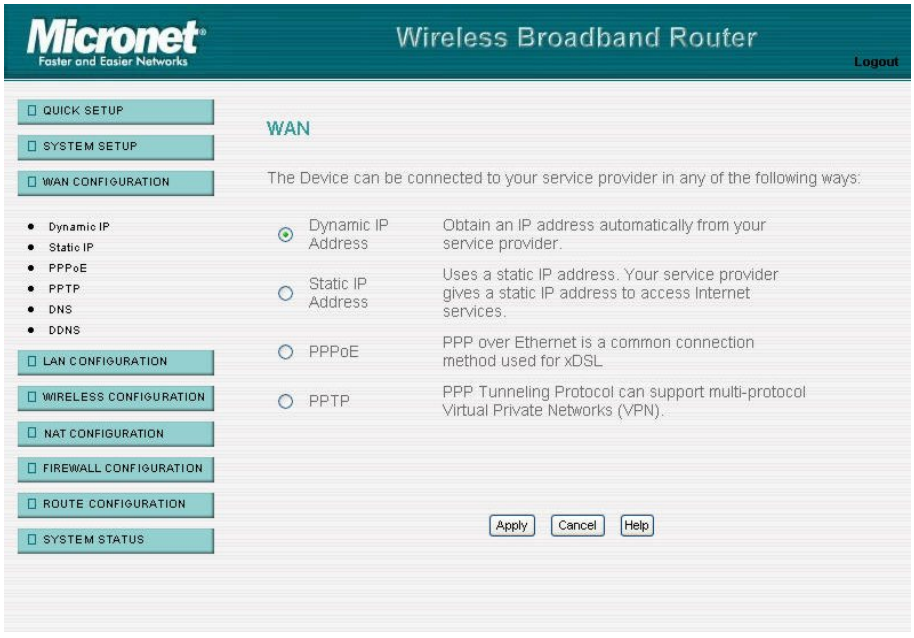
The function provides you to view all attempts made to gain access to your network. Click “**Download**” to save or open system log file. Clicking the “**Refresh**” button allows you to view the current status. The “**Clear**” button will clear all records saved in SP916GL.

3.2.7 System Reset


Micronet
Faster and Easier Networks
Wireless Broadband Router
Logout
QUICK SETUP
SYSTEM SETUP
Host Name Setting
System Time
Administrator Setting
Firmware Upgrade
Configuration Tools
System Log
System Reset
WAN CONFIGURATION
LAN CONFIGURATION
WIRELESS CONFIGURATION
NAT CONFIGURATION
FIREWALL CONFIGURATION
ROUTE CONFIGURATION
SYSTEM STATUS
Reset Wireless Router
In the event that the Wireless Router stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the "Reset" button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking.
Reset
Help

In the event that the SP916GL stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the "**Reset**" button below. You will be asked to confirm your decision.

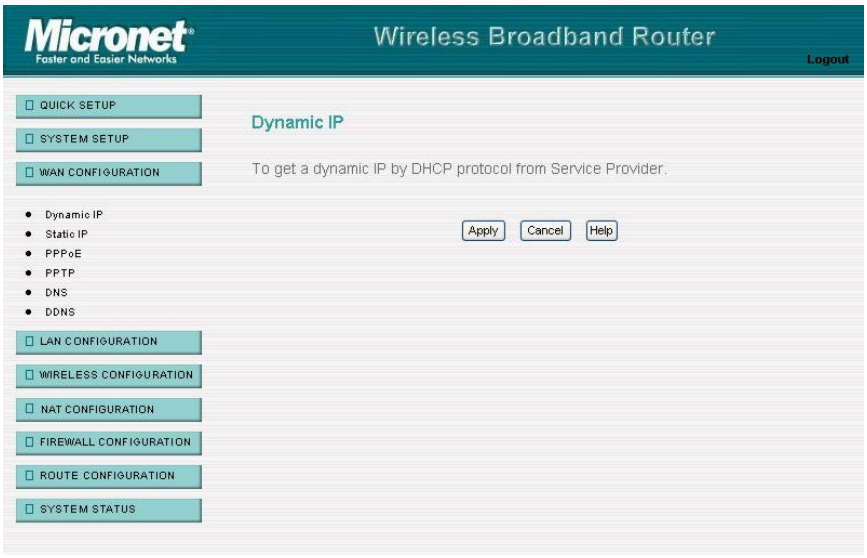
3.3 WAN Configuration Setting



SP916GL can be connected to your service provider in the following ways: “**Dynamic IP Address**”, “**Static IP Address**”, “**PPPoE**”, “**PPTP**”, ”**DNS**” and “**DDNS**” . You must confirm with your service provider on the detail information before configuration.

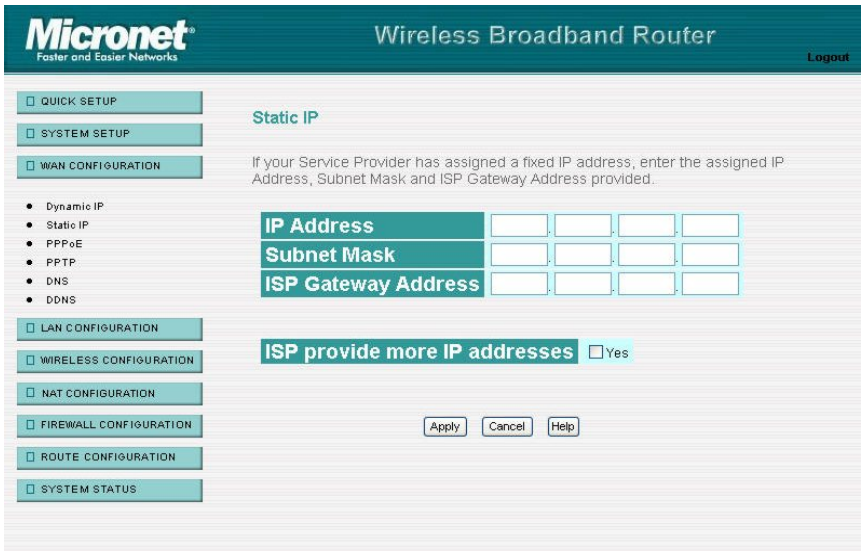
3.3.1 Dynamic IP Address:

This function will obtain an IP address from service provider automatically. Click “**Apply**” button below.



3.3.2 Static IP Address:

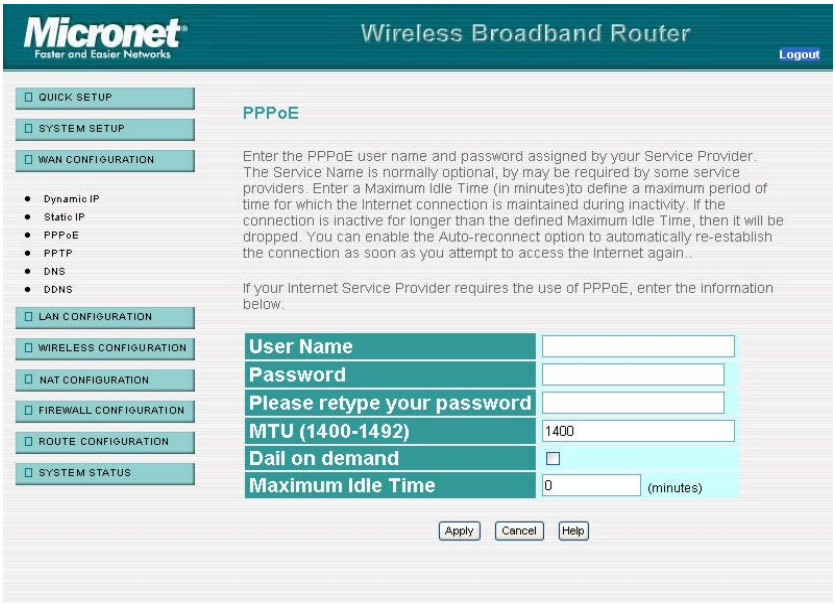
It allows you to use a static IP address in SP916GL. Your service provider gives a static IP address to access Internet services. After you enter the “**IP Address**”, “**Subnet Mask**”, and “**ISP Gateway Address**”



Note: “The ISP provide more IP address” will only provide you the IP address in the same Subnet Mask and ISP Gateway Address.

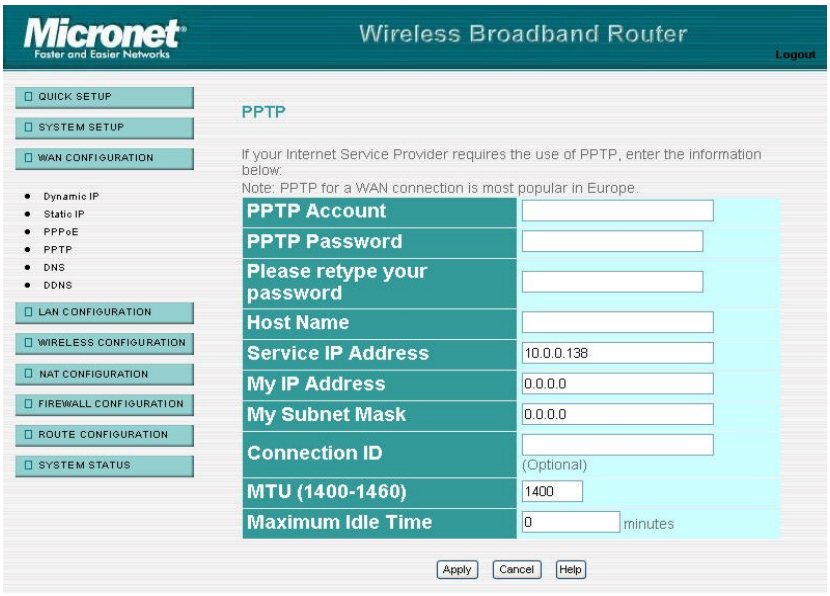
3.3.3 PPPoE:

PPP over Ethernet is a common connection method used for xDSL. You must enter the "**User Name**" and "**Password**" provided by your Internet Service Provider (ISP). You could set the **MTU** from 1400 to 1492. The default is 1400.


Micronet
Faster and Easier Networks
Wireless Broadband Router
Logout
QUICK SETUP
SYSTEM SETUP
WAN CONFIGURATION
Dynamic IP
Static IP
PPPoE
PPTP
DNS
DDNS
LAN CONFIGURATION
WIRELESS CONFIGURATION
NAT CONFIGURATION
FIREWALL CONFIGURATION
ROUTE CONFIGURATION
SYSTEM STATUS
PPPoE
Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, by may be required by some service providers. Enter a Maximum Idle Time (in minutes)to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the defined Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again..
If your Internet Service Provider requires the use of PPPoE, enter the information below.
User Name
Password
Please retype your password
MTU (1400-1492)
1400
Dail on demand
Maximum Idle Time
0
(minutes)
Apply
Cancel
Help

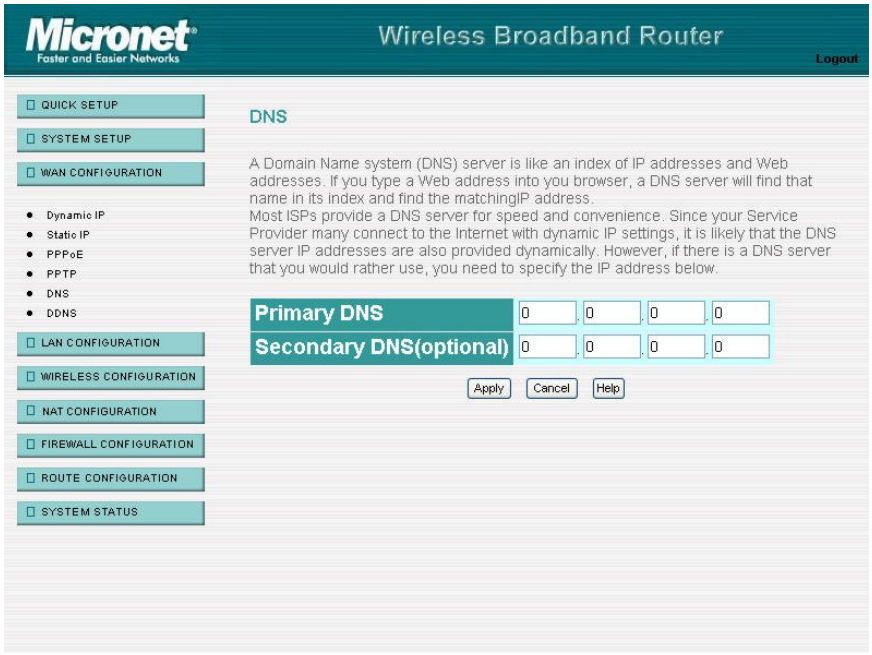
3.3.4 PPTP:

Point-to-Point Tunnel Protocol is a connection method used for specific area. You must enter the "**PPTP Account**", "**PPTP Password**" and "**Service IP Address** " provided by your ISP. Enter SP916GL IP address and Subnet Mask into the "**My IP Address**" and "**My Subnet Mask**" fields. Click "**Apply**" to continue.



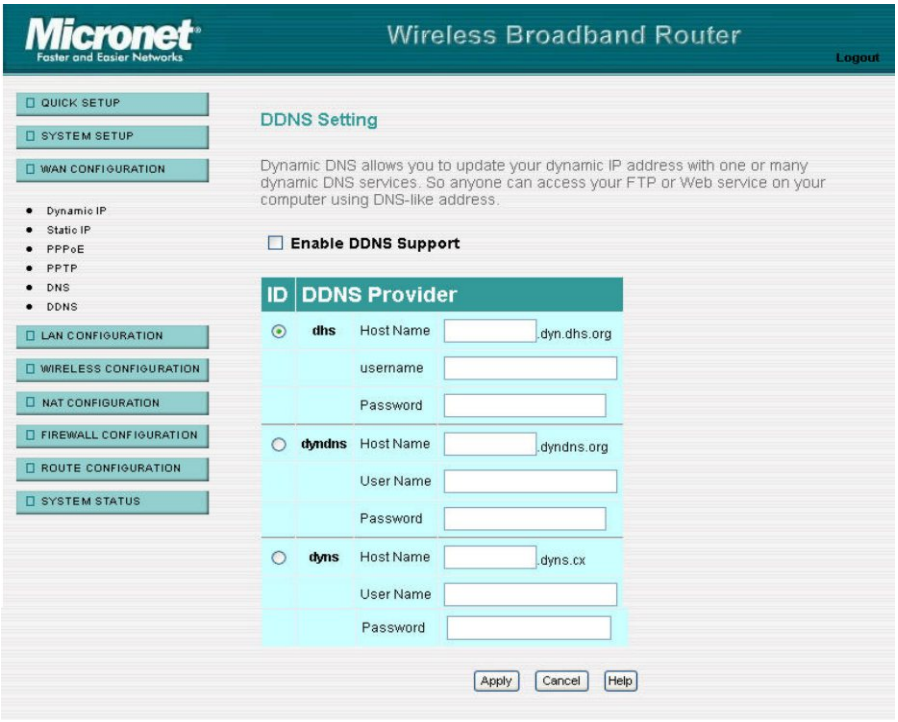
3.3.5 DNS:

A Domain Name system (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into you browser, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since many Service Providers connect to the Internet with dynamic IP settings, it is likely that the DNS server IP addresses are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address below.


Micronet
Faster and Easier Networks
Wireless Broadband Router
Logout
QUICK SETUP
SYSTEM SETUP
WAN CONFIGURATION
Dynamic IP
Static IP
PPPoE
PPTP
DNS
DDNS
LAN CONFIGURATION
WIRELESS CONFIGURATION
NAT CONFIGURATION
FIREWALL CONFIGURATION
ROUTE CONFIGURATION
SYSTEM STATUS
DNS
A Domain Name system (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into you browser, a DNS server will find that name in its index and find the matchingIP address.
Most ISPs provide a DNS server for speed and convenience. Since your Service Provider many connect to the Internet with dynamic IP settings, it is likely that the DNS server IP addresses are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address below.
Primary DNS
Secondary DNS(optional)
Apply
Cancel
Help

3.3.6 DDNS:

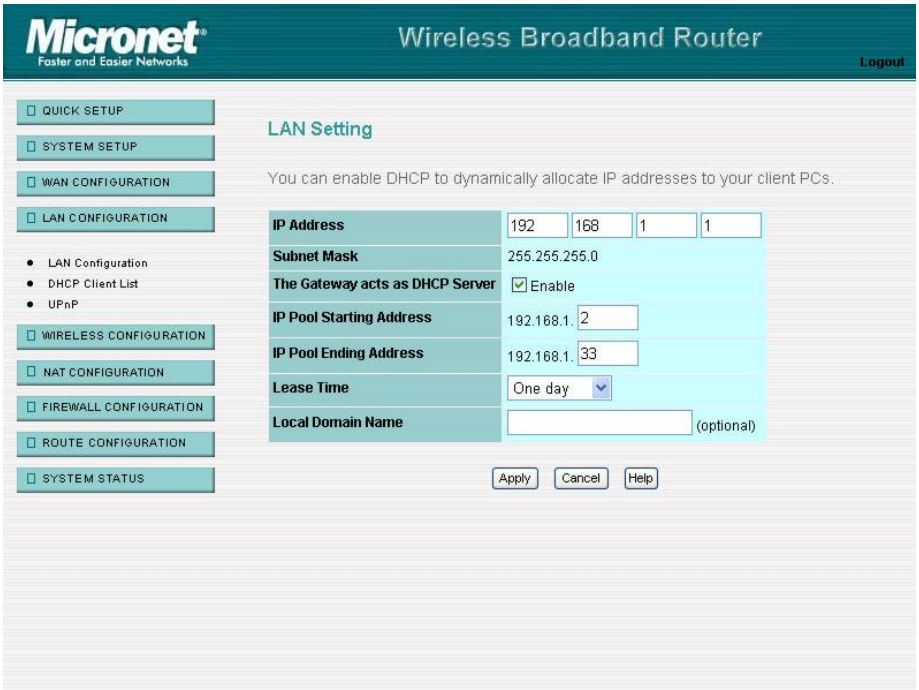
Dynamic DNS allows you to update your dynamic IP address with one or many dynamic DNS services. So anyone can access your FTP or Web service on your computer using DNS-like address. This allows the DDNS server to know what your current IP address is when you are on-line. You firstly need to register your preferred DNS on the DDNS providers include 3 types: "**dhs** ", "**dyndns**"and "**dyns** ". Then, please fill the related information in the below fields: "**Host Name**", "**User Name**"and "**Password**". You must check the "**Enable DDNS Support**" checkbox to enable the service. After you complete the configuration, you must remember to click "**Apply**" to continue.



3.4 LAN Configuration Setting

3.4.1 LAN Configuration:

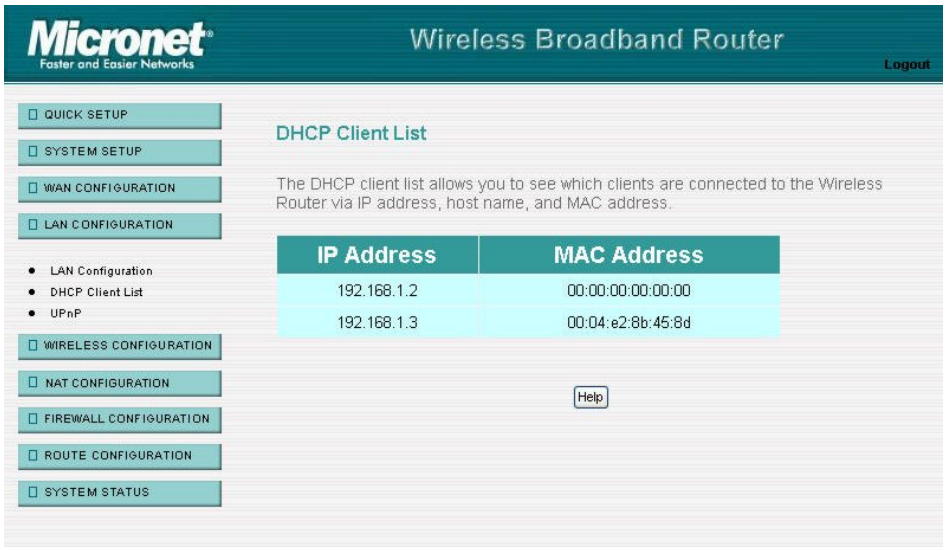
The '**LAN Settings**' option enables you to assign IP address to the router. If the DHCP Server is selected, the SP916GL will auto assign the IP address to the PC which connect to the SP916GL and setting it as a DHCP client.



Note: SP916GL has DHCP server internal. You could enter a DHCP range and assign IP address to client automatically. The Range is from 2 to 254. You could set the DHCP client Lease Time. Then you could type the local domain name of the network in the “Local Domain Name” text box. This item is optional.

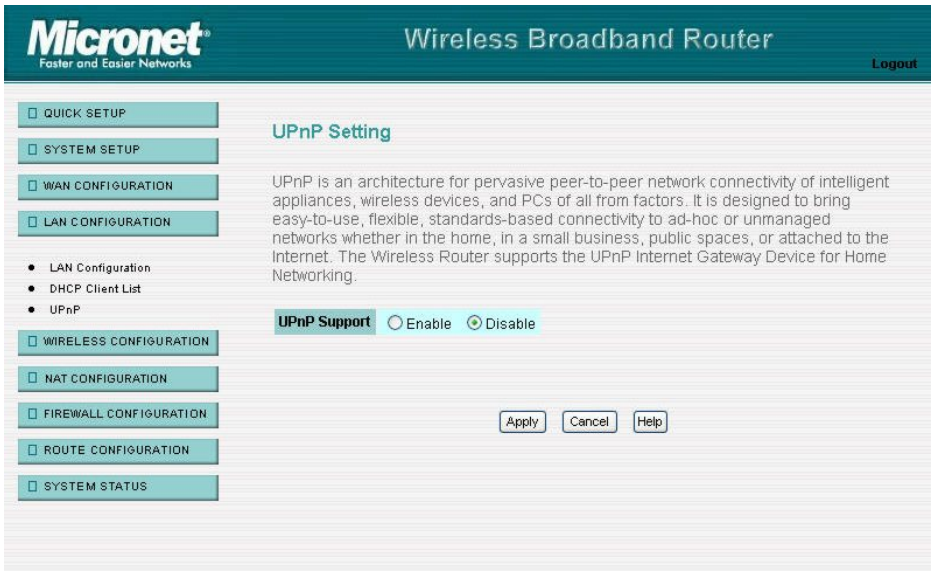
3.4.2 DHCP Client List:

The DHCP client list allows you to see which clients are connected to the router via **IP address** and **MAC address**.



3.4.3 UPnP configuration:

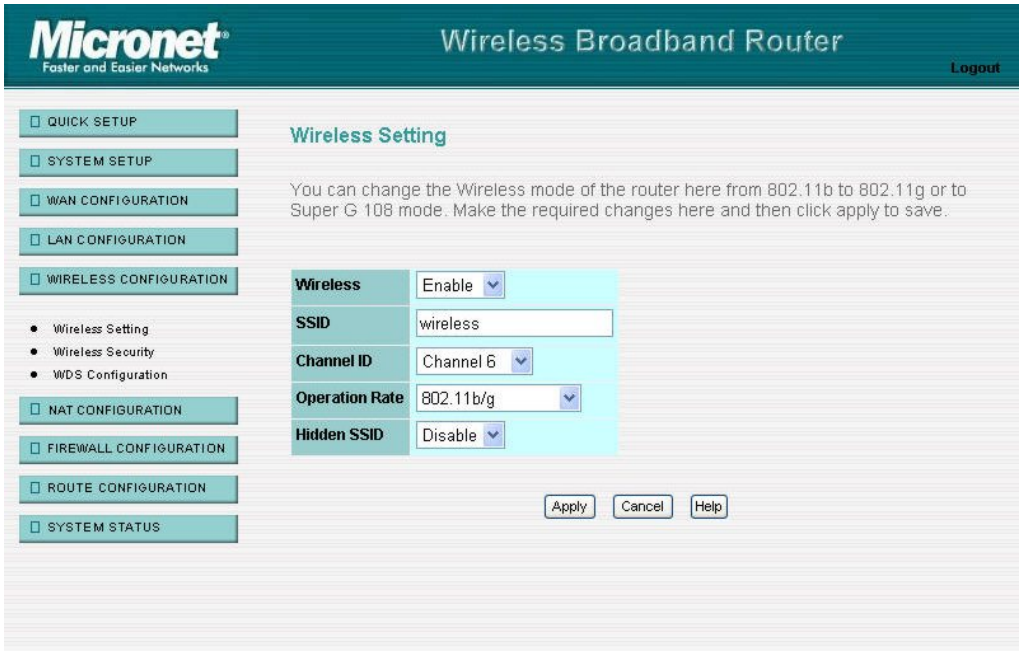
UPnP is architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices and PCs of all forms. You can **Enable** or **Disable** the UPnP function. SP916GL supports the UPnP Internet Gateway Device for Home Networking.


Micronet
Faster and Easier Networks
Wireless Broadband Router
Logout
QUICK SETUP
SYSTEM SETUP
WAN CONFIGURATION
LAN CONFIGURATION
LAN Configuration
DHCP Client List
UPnP
WIRELESS CONFIGURATION
NAT CONFIGURATION
FIREWALL CONFIGURATION
ROUTE CONFIGURATION
SYSTEM STATUS
UPnP Setting
UPnP is an architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices, and PCs of all from factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet. The Wireless Router supports the UPnP Internet Gateway Device for Home Networking.
UPnP Support
Enable
Disable
Apply
Cancel
Help

3.5 Wireless Configuration Setting

Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE802.11b/g wireless network adaptor to connect to your Intranet. It supports WEP encryption and MAC address filter to enhance the security of your wireless network.

3.5.1 Wireless Setting:



SSID: The identifier for the network. You can change the SSID. Only devices with the same SSID can interconnect.

Channel ID: The channel number used for networking. The channel setting of the wireless devices within a network should be the same.

Note: When operation rate set to Super G or Auto, the channel ID will fix in channel 6.

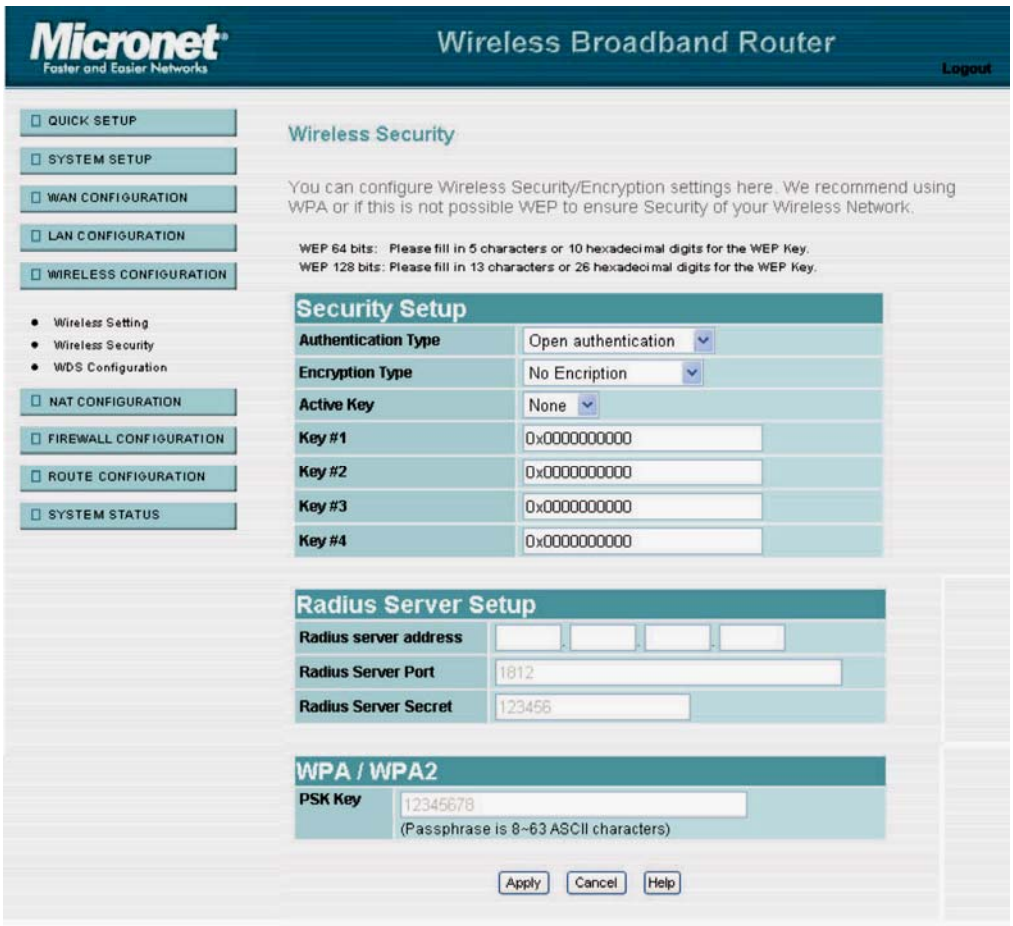
Operation Rate: SP916GL supports 802.11g, Super G (static) and Super G (dynamic).

Hidden SSID: You could enable or disable the function to hide the SSID of SP916GL in WLAN. The default is "**Disable**".

Click "**Apply**" to continue.

3.5.2 Wireless Security Setting:

SP916GL provides several wireless security setting. The available Authentication type includes “**Open system**”, “**Shared key**”, “**WPA-802.1x**”, “**WPA-PSK**”, “**WPA2-802.1x**” and "**WPA2-PSK**". You can configure wireless security/encryption setting here.



Encryption: To enable WEP, WPA, WPA2 and WPA2 Mixed encryption modes, select the option in the drop list. If you select none, all data will be transmitted without Encryption and every station can access the router.

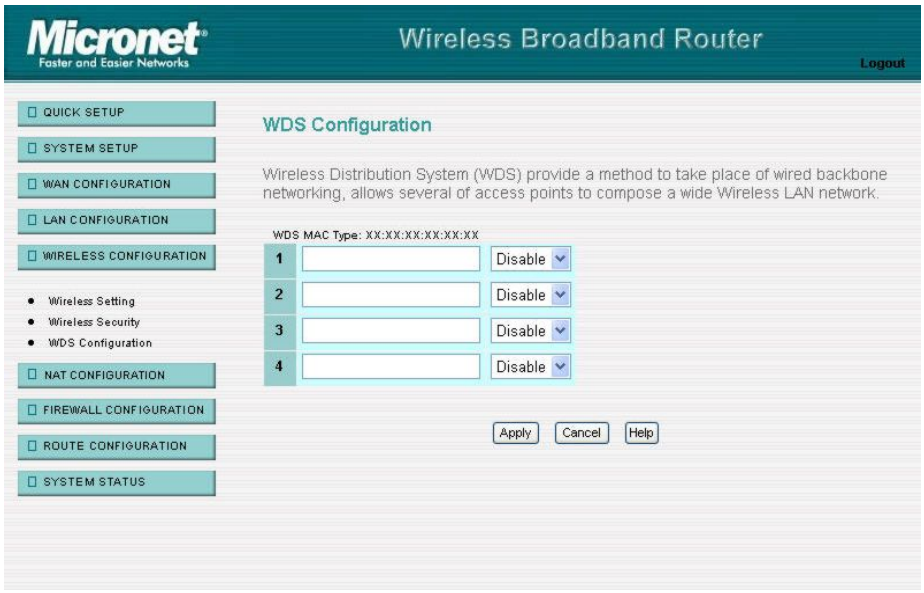
Key 1 ~ Key 4: Enables you to create an encryption scheme for Wireless LAN transmissions. Manually enter a set of values for each key. Select which key you want to use by clicking the radio button next to the key. Click Clear to erase key values.

RADIUS Sever Setup: If you use RADIUS Sever to ensure your security, you have to set up the parameters in this item. To set up, enter the same **Port**, **IP address** and **Radius Server Secret** as your RADIUS server. If WPA or 802.1X is selected. Please set the length of the encryption key and the parameters for the RADIUS server. If **WPA-PSK** is selected, please set the **PSK Key** in the pass phrase field. The length should be 8 characters at least.

Note: As soon as 802.1X security is enabled, all the wireless client stations that are connected to the Router currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected.

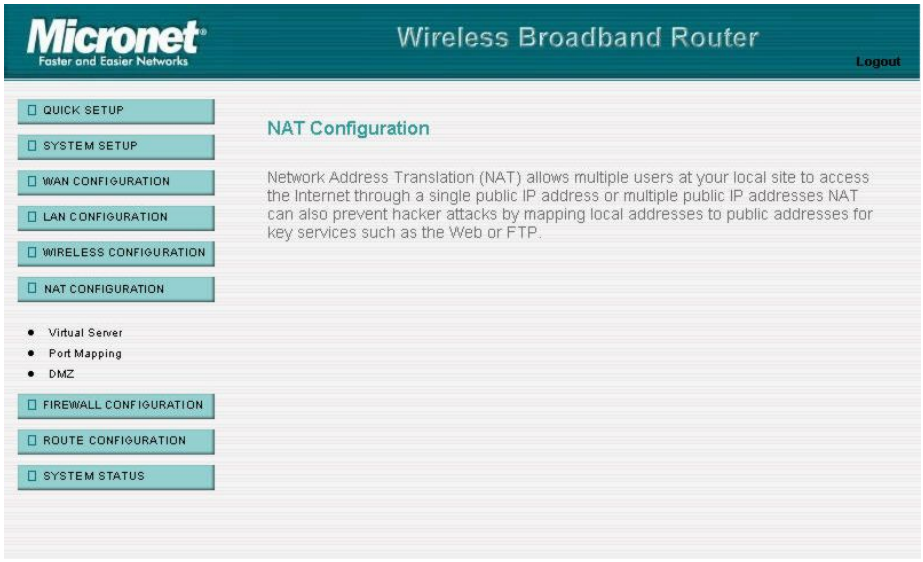
3.5.3 WDS Configuration Setting:

Wireless Distribution System allows SP916GL to communicate with other SP916GLs wirelessly. To make it work, you must ensure that these APs and the Router are in the same Channel and then add these APs MAC Address and Comment values into the WDS list. Enter the MAC Address of another AP you want to connect to and choose **Enable** to enable the WDS link. Click the **Apply** button to save the setting.



3.6 NAT Configuration Setting

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses NAT can also prevent hacker by mapping local addresses to public address.


Micronet
Faster and Easier Networks
Wireless Broadband Router
Logout
QUICK SETUP
SYSTEM SETUP
WAN CONFIGURATION
LAN CONFIGURATION
WIRELESS CONFIGURATION
NAT CONFIGURATION
Virtual Server
Port Mapping
DMZ
FIREWALL CONFIGURATION
ROUTE CONFIGURATION
SYSTEM STATUS
NAT Configuration
Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

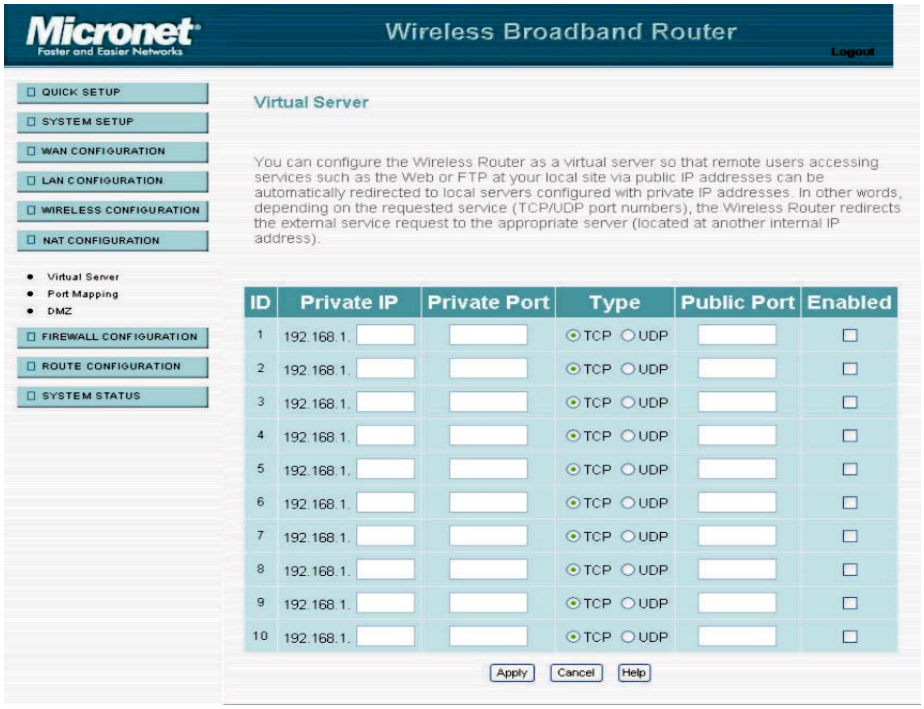
3.6.1 Virtual Server Setting:

This screen enables you to create a virtual server via SP916GL. If SP916GL is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The router redirects the request via the protocol and port numbers to the correct LAN server. The Virtual Sever profiles are listed in the table at the bottom of the page. Enter "**Private IP**", "**Private Port**", "**Type**", "**Public Port**" in the appropriate fields and check the "**Enabled**" checkbox. After you complete the configuration, remember to click "**Apply**" to continue.

Note: To select items in the table at the bottom, click anywhere in the item. When the line is selected, the fields automatically load the parameters for the item for you to edit.

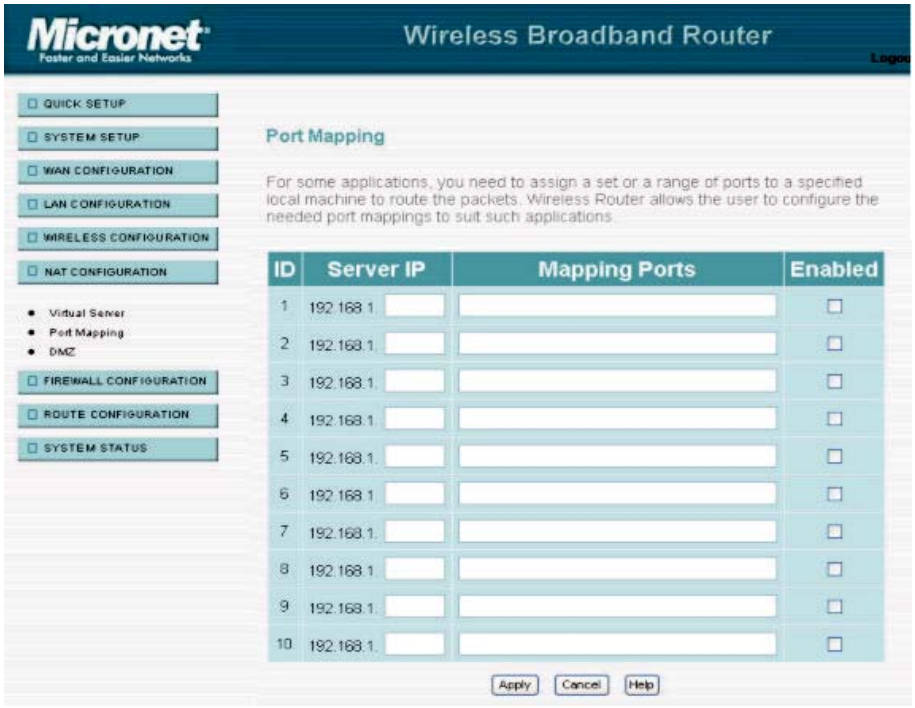
Type: Select the protocol (TCP or UDP) you want to use for the virtual server. Private Port: Type the port number of the computer on the LAN that is being used to act as a virtual server.

Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.


Micronet
Faster and Easier Networks
Wireless Broadband Router
Logout
QUICK SETUP
SYSTEM SETUP
WAN CONFIGURATION
LAN CONFIGURATION
WIRELESS CONFIGURATION
NAT CONFIGURATION
Virtual Server
Port Mapping
DMZ
FIREWALL CONFIGURATION
ROUTE CONFIGURATION
SYSTEM STATUS
Virtual Server
You can configure the Wireless Router as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port numbers), the Wireless Router redirects the external service request to the appropriate server (located at another internal IP address).
ID
Private IP
Private Port
Type
Public Port
Enabled
1 192.168.1. TCP UDP
2 192.168.1. TCP UDP
3 192.168.1. TCP UDP
4 192.168.1. TCP UDP
5 192.168.1. TCP UDP
6 192.168.1. TCP UDP
7 192.168.1. TCP UDP
8 192.168.1. TCP UDP
9 192.168.1. TCP UDP
10 192.168.1. TCP UDP
Apply
Cancel
Help

3.6.2 Port Mapping Setting:

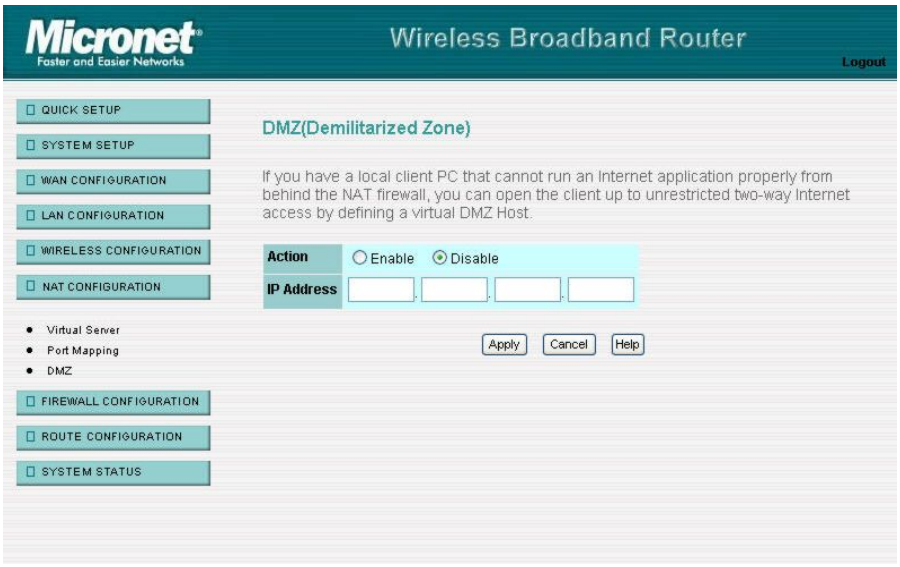
For some applications, you need to assign a set or a range of ports to a specified local machine to route the packets. SP916GL allows the users to configure the needed mappings to suit such application. You must enter the **Server IP** and **Mapping Ports**. After you complete the setting then please remember to check the **Enabled** checkbox and click "**Apply**" to continue.



3.6.3 DMZ Setting:

This screen enables you to create a DMZ for those computers that cannot access Internet applications properly through the router and associated security settings.

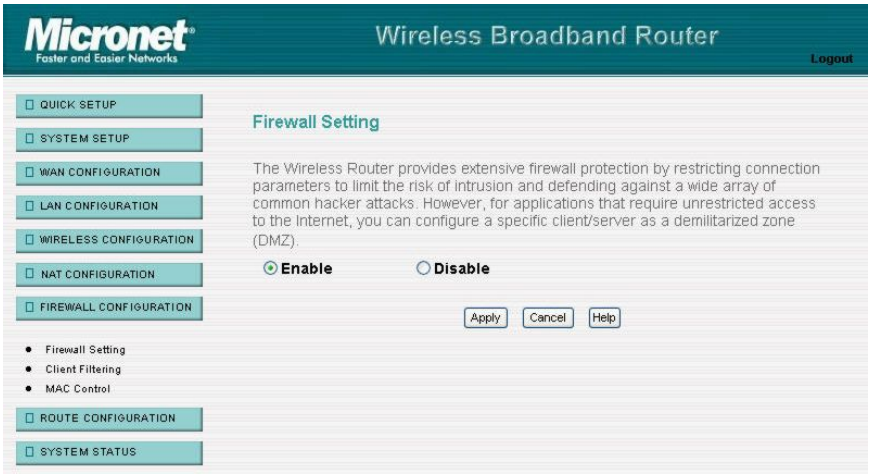
Note: Adding clients to the DMZ exposes the client to security risks such as viruses and unauthorized access.



3.7 Firewall Configuration

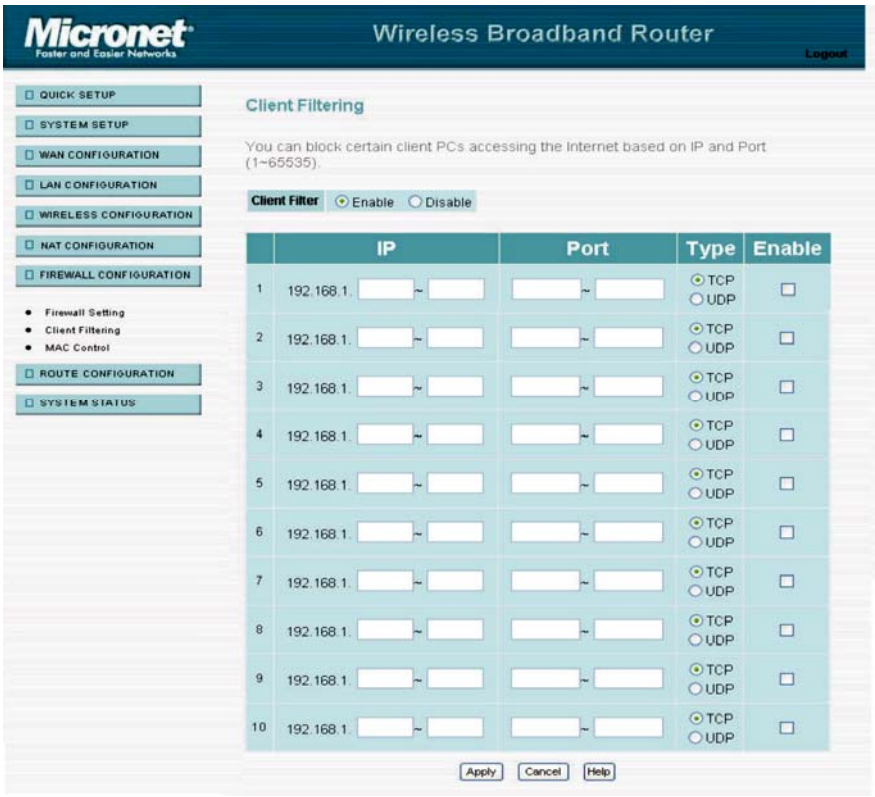
3.7.1 Firewall Setting:

SP916GL provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a DeMilitarized Zone (DMZ)



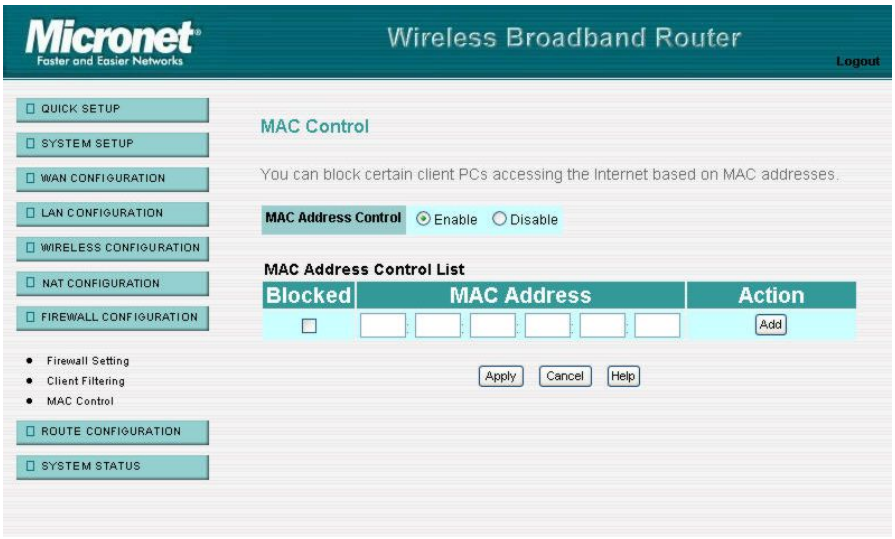
3.7.2 Client Filtering:

SP916GL could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet via **Client Filtering**.



3.7.3 MAC Control:

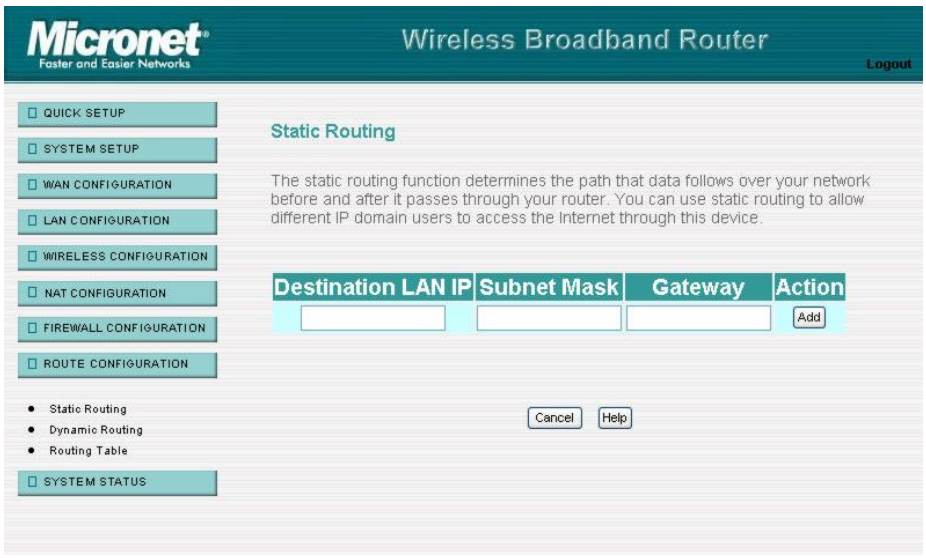
SP916GL could filter the outgoing packets for security or management consideration based on **MAC address**.



3.8 Route Configuration

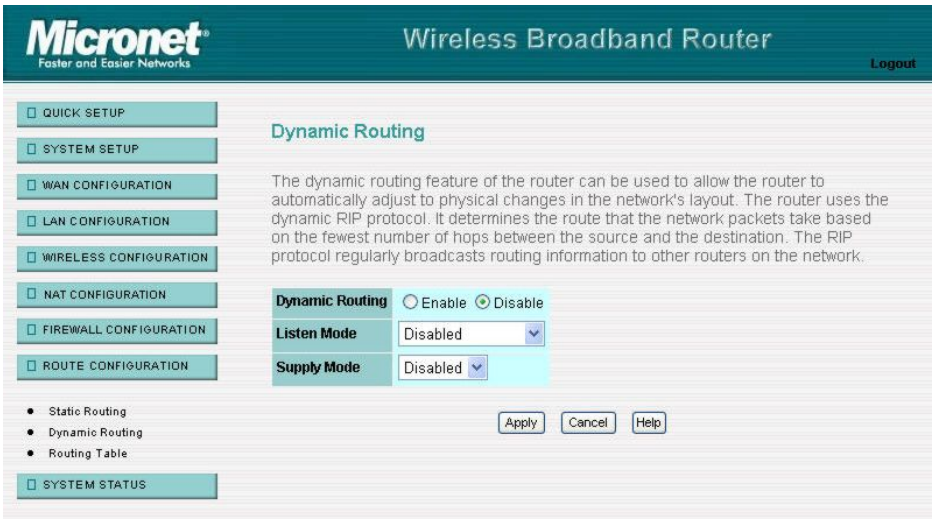
3.8.1 Static Routing:

The static routing function determines the path that router follows over your network before and after it passes through SP916GL. You can use static routing to allow different IP domain users to access the Internet through this device. After you enter the parameter, remember to click "**Add**" button.



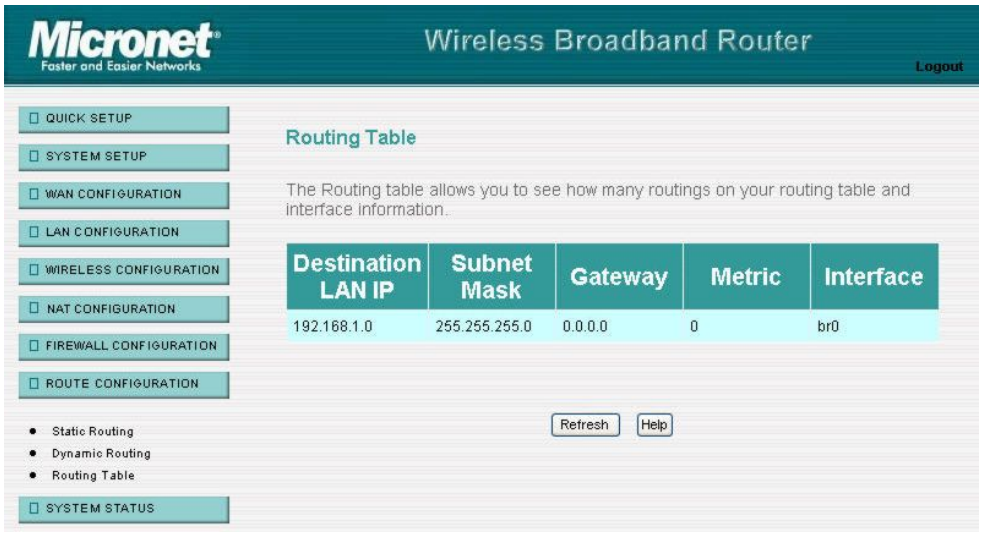
3.8.2 Dynamic Routing:

The dynamic routing feature of the router can be used to allow the router to automatically adjust to physical changes in the network's layout. The router uses the dynamic RIP protocol. It determines the route that the network packets take based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.


Micronet
Faster and Easier Networks
Wireless Broadband Router
Logout
QUICK SETUP
SYSTEM SETUP
WAN CONFIGURATION
LAN CONFIGURATION
WIRELESS CONFIGURATION
NAT CONFIGURATION
FIREWALL CONFIGURATION
ROUTE CONFIGURATION
Static Routing
Dynamic Routing
Routing Table
SYSTEM STATUS
Dynamic Routing
The dynamic routing feature of the router can be used to allow the router to automatically adjust to physical changes in the network's layout. The router uses the dynamic RIP protocol. It determines the route that the network packets take based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.
Dynamic Routing
Enable
Disable
Listen Mode
Disabled
Supply Mode
Disabled
Apply
Cancel
Help

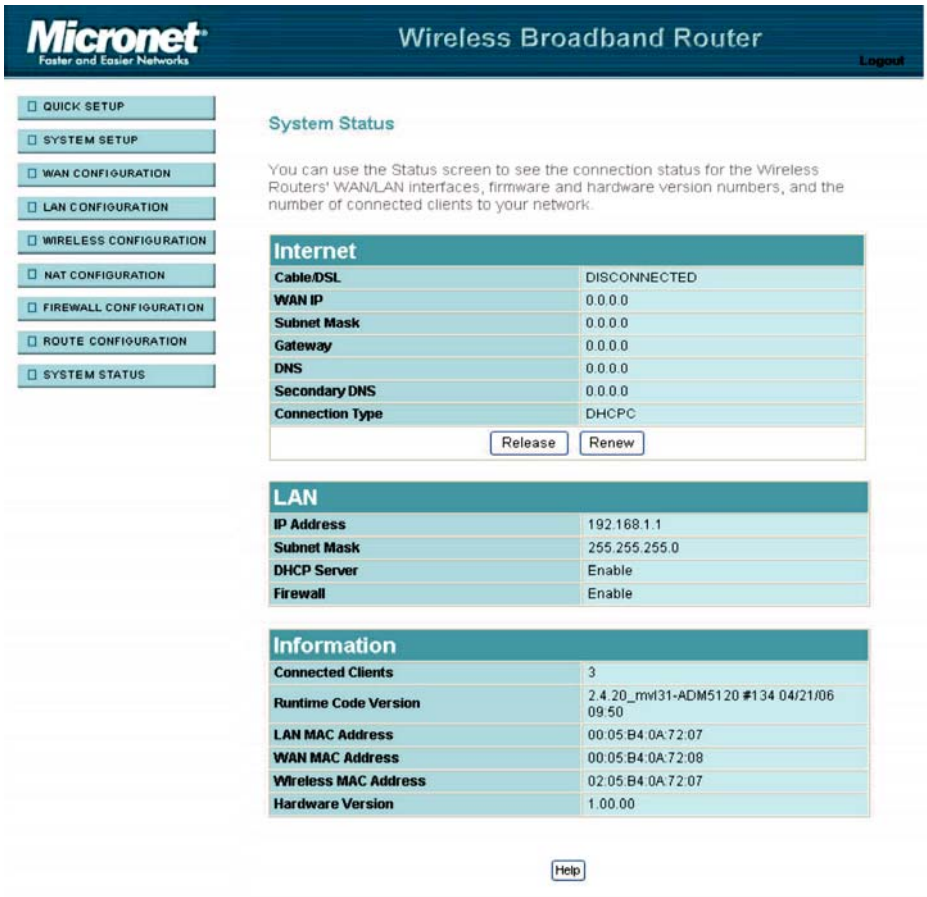
3.8.3 Routing Table:

The Routing table allows you to see the routings on your routing table and interface information.



3.9 System Status

The System Status page shows the WAN, LAN and router's firmware version



4 Glossary

Access Point
A transceiver or radio component in a wireless LAN that acts as the transfer point between wired and wireless signal, and vice versa.
Authentication
Authentication refers to the verification of a transmitted message's integrity.
DMZ
DMZ (DeMilitarized Zone) is a part of a network that is located between a secure LAN and an insecure WAN. DMZs provide a way for some clients to have unrestricted access to the Internet.
DHCP
DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.
DNS
DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name.
Domain Name
The domain name typically refers to an Internet site address.
DTIM
DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages.
Filter
Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.
Firewall
Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN.
Firmware
Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface.
Fragmentation
Fragmentation refers to the breaking up of data packets during transmission.
FTP
FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for transferring large files or uploading the HTML pages for a Web site to the Web server.
Gateway
Gateways are computers that convert protocols enabling different networks,

applications, and operating systems to exchange information.

Host Name

The name given to a computer or client station that acts as a source for information on the network.

HTTP

HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example, http://www.yahoo.com).

ICMP

ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available).

IP

IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery.

IP Address

The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189).

ISP

An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN

LANs (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and communications links such as the router.

MAC Address

A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.

Metric

A number that indicates how long a packet takes to get to its destination.

MTU

MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets.

NAT

NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa).

NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

(Network) Administrator

The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity.

NTP

NTP (Network Time Protocol) is used to synchronize the realtime clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC).

Packet

A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address.

Ping

Ping (Packet INternet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging.

Port

Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered.

PPPoE

PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.

PPTP

Point-to-Point Tunneling Protocol uses TCP to deal data for tunnel maintenance, and uses PPP for sum up the information carried within the tunnel. The data carried within the tunnel can be compressed or encrypted. The encryption method used is RSA RC4. PPTP can operate when the protocol is supported only on the client and the server located on the other end that the client is corresponds with. No support is essential from any of the routers or servers within the network the two PCs are connecting across.

Protocol

A protocol is a rule that governs the communication of data.

RIP

RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

51

RTS

RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server

Servers are typically powerful and fast machines that store programs and data.

The programs and data are shared by client machines (workstations) on the network.

SMTP

SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

Subnet Mask

Subnet Masks are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP address to determine whether to accept or reject the packet.

SysLog Server

A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.

TCP

(Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in real-time video and audio transmission). The IP component of TCP/IP provides data routability, meaning that data packets contain the destination station and network addresses, enabling TCP/IP messages to be sent to multiple networks within the LAN or in the WAN.

UDP

(User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate delivery isn't necessary (for example, real-time video and audio where packets can be dumped as there is no time for retransmitting the data).

Virtual Servers

Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WAN

WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building).